CITY
OF
SCOTTSDALE

Office of the City Auditor

Internet Security Testing
Interim Report No. 9810.B

March 9, 2000

Reliance on the City's computer networks and the Internet has risen rapidly without the same emphasis on enterprise security. In response, the Chief Information Officer is requesting financial assistance to strengthen information systems security.

"Most Livable City"

U.S. Conference of Mayors

OFFICE OF
CITY AUDITOR

7440 E. FIRST AVE
SCOTTSDALE, AZ 85251

(480) 312-7756 PHONE
(480) 312-2634 FAX

March 9, 2000

To the Most Honorable Sam Kathryn Campana, Mayor
and the Members of the Scottsdale City Council

This is an interim report on our evaluation of internal controls and security of the City's information system assets. The evaluation is being completed using control objectives outlined by the Information Systems Audit and Control Foundation. Results of segments will be issued as interim reports with all information compiled and presented at the conclusion of the work. This project was approved for inclusion on the City Auditor's Fiscal Year 1998/99 Audit Plan.

This report discusses the need for citywide policies and procedures as well as a full-time information system security function. Also included in the report are the findings and recommendations of an outside computer security firm hired to evaluate network security. The executive summary presented by the consultant is included as Appendix A. For security purposes, IP address ranges have been eliminated.

The conclusions of the outside consultant were provided to Information Systems management and the Technology Board of Directors at the conclusion of the work. As well, this report was provided to management for review and comment. Written management responses are included in Appendix B.

Respectfully submitted,

Cheryl Lee Barcala

Cheryl Barcala, CPA, CIA, CFE, CGFM, CISA
City Auditor

Internet Security Testing
Report No. 9810B

Action Plan

	Management Response		Implementation Status		
No.	AGREE	DISAGREE	UNDERWAY	PLANNED	RECOMMENDATIONS
1	X			X	The Chief Information Officer (CIO) should develop a citywide policy statement establishing a positive control environment and addressing aspects such as the code of conduct governing use and security of information system assets, management responsibility and user accountability, and management philosophy and direction regarding IS.
2	X		X		The CIO should create a full-time information system security position directed to implement a security program including:
				X	• Development of citywide security policies to ensure appropriate preventive measures, timely identification of errors or irregularities, limitation of losses, and timely restoration. This policy should address purpose and objectives, management structure, scope, assignment of responsibility, and penalties and disciplinary actions associated with failing to comply.
				X	• Development and implementation of an awareness program structured to communicate the security policy to all system users as a means of conveying the benefit of information system security to the organization, employees, and citizens. This awareness program should be supplemented with annual training to address security practices including ethical use of information system assets, and appropriate steps to protect against system failures and breaches.
				X	• Development and implementation of a monitoring program to detect attempted system intrusions.
				X	• Development of a CERT to appropriately address system security issues such as denial of service attacks and security breaches.
3	X			X	The CIO should develop a program to ensure independent vulnerability assessments at least biennially.

EXECUTIVE SUMMARY

The City has implemented a state of the art computer network system as part of the City's Information Systems (IS) strategic plan. The goal of this network system is to be reliable, secure, scaleable, and easy to use. IS staff work diligently to maintain appropriate levels of security through the use of firewalls and other appropriate controls. However, given the rapidly evolving nature of computer systems and the increasing risk of exposure to more sophisticated computer viruses and trespassers, periodic evaluations of system security controls is an important part of a network security system.

In the Spring of 1999, IS management and City Auditor staff discussed information system assets security. IS staff were in the process of implementing a new firewall and several departments were considering e-business applications to offer services through the Internet. As a result, a joint project was initiated to undertake a vulnerability assessment. The assessment was designed to evaluate system configuration, look for appropriate security patches, assess the adequacy of password protection, and identify other potential threats. As well, the consultant evaluated existing policies and procedures and the structure of the security program as a means of reducing risk from internal vulnerabilities. To supplement this assessment, our office initiated discussions regarding security control objectives.

Results in Brief

Based on our work, and supplemented with the results of the vulnerability assessment, we believe that security controls need to be enhanced. While IS staff have taken appropriate steps to control security as evidenced by the external firewall and other security measures such as user authentication (IDs and passwords), these controls by themselves are not sufficient.

To ensure an adequate control environment, an organization needs a policy statement that sets the framework for control as well as the tone for a positive control environment. System users must be educated through an awareness program to establish the responsibility for ethical use and security of the system. While there are many informal policies governing security of information system assets, they have not been developed, documented, or communicated sufficiently throughout the organization.

In addition to policy and education programs, the City needs to establish an organized system security function. The system security function serves to provide the appropriate level of direction, awareness, and response necessary to protect the City's information system assets. As well, it serves as the means to implement system security monitoring, a proactive effort to protect the system. By using software programs that identify potential attempts to gain unauthorized access to the City network, intrusions can often be stopped before damage occurs.

As part of the vulnerability assessment, IS and City Auditor staff evaluated the monitoring software used by the outside consultant. Purchase and implementation of the software is included in the recommendations set out below.

We recommend:

1. Development of a citywide policy statement establishing a positive control environment and addressing aspects such as the code of conduct governing use and security of information system assets, management responsibility and user accountability, and management philosophy and direction regarding IS.

2. Creation of a full-time information system security position directed to implement a security program including:

   - Development of citywide security policies to ensure appropriate preventive measures, timely identification of errors or irregularities, limitation of losses, and timely restoration. This policy should address purpose and objectives, management structure, scope, assignment of responsibility, and penalties and disciplinary actions associated with failing to comply.

   - Development and implementation of an awareness program structured to communicate the security policy to all system users as a means of conveying the benefit of information system security to the organization, employees, and citizens. This awareness program should be supplemented with annual training to address security practices including ethical use of information system assets and appropriate steps to protect against system failures and breaches.

- Development and implementation of a monitoring program to detect attempted system intrusions.
- Development of a Computer Emergency Response Team (CERT) to appropriately address system security issues such as denial of service attacks and security breaches.

3. Development of a program to ensure independent vulnerability assessments at least biennially.

IS management agrees with these recommendations and has submitted a budget request for consideration in the second year budget adjustments. This request will provide funding for a full-time information system security position, and sufficient funds to implement policy development and develop the initial awareness program. Funds are also included to implement a structured monitoring program.

Background

Over the past decade, the City has moved aggressively towards implementation of a strategic plan to move from a mainframe computing environment to a client/server based network. This decision empowered end users by placing technology directly within departments and expanded the ability to access resources such as the Internet. The advent of more cost-effective computer resources, fueled by the rapidly changing environment, created enormous opportunities to expand the role technology played within the organization.

This expanded role also created greater dependency on the computer resources and increased the risk of greater vulnerabilities and threats. Prior to a distributed computer environment, computer security controls focused on maintaining security to the room where the computer was housed. Access to the information was closely controlled through established passwords and a structure that required someone to have physical access to the computer before attempting to breach the password security. Systematic back-up processes ensured that recovery of data would be possible should an error or other event damage data.

This control environment no longer exists. Access to the computer resources is no longer restricted and data is kept on desktop computers, no longer part of the systematic back-up. System security, in most instances, is provided by establishing user profiles, controlled by password authentication, as a means of granting access to data or resources. With access to the City network, a user can easily navigate and use any computing resource necessary to conduct City business. Dial-in connections allow users to access the City network from remote locations. The Internet provides opportunities for citizens to obtain data regarding City business and e-mail City staff.

As the City moves towards more opportunities for e-business, there will be a greater need for access to computer resources. These opportunities bring a requirement for greater system security. Each additional access point creates the potential for security breaches or accidental destruction of data.

The Information System Audit and Control Foundation, the research arm of the Institute of Information System Audit and Control (ISACA), recognized the need for greater control over information system assets. To address this need, ISACA sponsored Control Objectives for Information and Related Technology (COBIT). This document sets the framework for good control practices. It can also be used as a management self-evaluation tool. As well, it serves as the generally applicable and accepted audit guidelines for information system auditors when reviewing processes. As such, these guidelines were used when developing the objectives for this audit.

COBIT also recommends periodic vulnerability assessments. IS management agreed that the vulnerability assessment conducted during this review would serve to establish a baseline for future evaluations. IS staff assisted in establishing objectives for this assessment and evaluating the responses to the request for proposals.

This assessment was accomplished by loading monitoring software on selected City servers. This allowed an assessment of the firewall and 15 nodes of the City’s network. The security penetration assessment began October 19, 1999, with a preliminary report provided on October 22, 1999. The final written report was received November 1, 1999, and the exit meeting was conducted on December 7, 1999.

At the conclusion of the analysis, the outside consultant provided us with an executive summary of findings and recommendations (Appendix A) and detailed source documentation. In addition to the exit meeting, the consultants gave a presentation to the City of Scottsdale Technology Board.

Conclusion

The City does not have a documented citywide policy that sets out management responsibility for a positive control environment, nor does the City have a documented system security policy. User awareness programs do not exist and specific training regarding system security is not required before a user is granted access to City computing resources. System security is not monitored, other than as time is available, and an information system security position does not exist as a means of providing a citywide focus on good controls.

This environment does not provide the desired level of control. Our findings were also supported by the vulnerability assessment conducted by an outside consultant. This assessment found situations in which potential vulnerabilities, such as changing default passwords and accounts, had not been addressed. The outside consultant also recommended creation of a full-time information system security officer and establishing a security policy.

We believe these conditions exist as a result of the rapid changes in the computer environment. The focus on keeping up with the technology changes and user needs has left few resources available to fulfill the role of system security. Many of the conditions highlighted by the vulnerability assessment can be traced to limited staff resources available to address issues that staff are aware of or had not been able to document.

These issues are addressed in the following sections.

Framework and User Awareness

Information system security starts with the premise that control over information system assets and related technology is enhanced when senior management sets policies that communicate a positive control environment. This statement provides the framework and should address issues such as integrity, ethical values, competency of staff, management philosophy, operating style, accountability, attention, and direction. It serves to set the tone for compliance and the results for non-compliance.

The overall framework policy is supplemented with a security and internal control program that is developed based on overall business objectives. This program should be designed to minimize risk with preventative measures, timely identification of errors and irregularities, limitation of loss, and timely restoration in the event of a failure or breach. Required, periodic training programs increase awareness of appropriate security practices.

Currently neither the citywide policy statement nor the system security program exists. Staff operate with established practice based on individual knowledge and organizational support. As a result, practice varies from individual to individual depending on knowledge and departmental support.

System Vulnerability and Monitoring

The effectiveness of policies and procedures should be assessed periodically as a means of determining actual practice. As well, the system needs to be monitored to guard against potential intrusions. Response plans need to be developed to provide direction on how to deal with intrusions such as denial of service attacks or data recovery. These areas of expertise fall under the responsibility of an information system security position.

Monitoring software is considered an industry norm in the efforts to control access to computer systems. With implementation of a program, staff can conduct periodic internal assessments of passwords, security patches, and system configuration. The software also provides notice of attempts to gain unauthorized access to resources which can be used to re-direct suspicious traffic or deny access to resources. These preventative measures can reduce system risk.

Currently, system assessment and monitoring is a shared responsibility. IS staff work diligently towards addressing issues and attempt to reduce the exposure by controlling external access with the firewall. However, not all appropriate security issues such as renaming known accounts and requiring adequate passwords have been implemented. Staff must fit security related issues in along with other job duties such as network installation and Internet applications.

Independent Assessments

Internal monitoring programs also need to be supplemented with independent vulnerability assessments structured to look for weaknesses within the system. The assessment conducted as part of this review will serve as the baseline for future work. As part of an effective security program, periodic independent assessments should be required no less frequently than every other year.

The outside consultant concluded that information system controls, as currently structured, are below industry norms. The recommendations set out by the outside consultant included:

- Ensuring all available vendor patches and operating systems upgrades are installed.
- Limiting the number of services to the minimum required for business operations.
- Developing a password policy, assigning passwords to printers, requiring passwords on all systems, and changing known default passwords.
- Establishing an information system security position, creating policies, standards and procedures, and implementing a security program.
- Setting account controls, renaming known accounts, reviewing user access needs, protecting event logs, and enabling audit subsystems.

RECOMMENDATIONS

1. The Chief Information Officer (CIO) should develop a citywide policy statement establishing a positive control environment and addressing aspects such as the code of conduct governing use and security of information system assets, management responsibility and user accountability, and management philosophy and direction regarding IS.

2. The CIO should create a full-time information system security position directed to implement a security program including:

   - Development of citywide security policies to ensure appropriate preventive measures, timely identification of errors or irregularities, limitation of losses, and timely restoration. This policy should address purpose and objectives, management structure, scope, assignment of responsibility, and penalties, and disciplinary actions associated with failing to comply.
   - Development and implementation of an awareness program structured to communicate the security policy to all system users as a means of conveying the benefit of information system security to the organization, employees, and citizens. This awareness program should be supplemented with annual training to address security practices including ethical use of information system assets, and appropriate steps to protect against system failures and breaches.
   - Development and implementation of a monitoring program to detect attempted system intrusions.
   - Development of a CERT to appropriately address system security issues such as denial of service attacks and security breaches.

3. The CIO should develop a program to ensure independent vulnerability assessments at least biennially.

ABBREVIATED RESPONSE

IS management concurs with these recommendations and has submitted a budget request for consideration in the second year budget adjustments for a security position to properly secure and protect the City’s network.

APPENDIX A

Axent Technologies Report

Information Security Solutions Roadmap

Final Report for City of Scottsdale, Scottsdale, AZ

SCR-9909-06

Date: November 1, 1999
Version: 1.0

SECURE NETWORK CONSULTING, INC.
A subsidiary of Axent Technologies, Inc.

Contents

1. Introduction

This report presents the Information Security Solutions Roadmap developed by Secure Network Consulting, Inc. (SNCi) for the City of Scottsdale located in Scottsdale, AZ. SNCi developed the Roadmap on the basis of information collected onsite from 19 October to 22 October 1999.

In the Roadmap, SNCi describes information security vulnerabilities discovered, and presents prioritized recommendations for correcting these weaknesses. The Roadmap will provide the City of Scottsdale with a traceable plan for establishing an information security posture that is consistent with industry best practices.

1.1 Background and Objectives

The City of Scottsdale contracted with AXENT/SNCi for delivery of a Limited Express Vulnerability Assessment Service (LEVAS) between 19 October and 22 October 1999.

During the EVAS, SNCi used its information security expertise and employed proven information security assessment processes and products to:

- Assess system and network vulnerabilities that could be exploited to adversely impact critical information system resources identified by City of Scottsdale,

- Analyze the findings to determine methods for eliminating or mitigating the assessed vulnerabilities, and

- Develop and document prioritized recommendations for correcting assessed information.

1.2 Scope

The scope defined by City of Scottsdale identified the specific sites to be visited, as well as the specific host systems and subnets to be included in the assessment are identified in the tables below.

Table 1 describes the hosts assessed by SNCi and the function of each host.

Table 1. Host-level Sample Set

Host Name	IP Address and Operating System	Critical Function
Auditorapps01	[redacted]	Audit Server
1cctransapps01	[redacted]	Weather Data Server
Scapayrolapps01	[redacted]	Payroll
Chimg01	[redacted]	City Clerk Image
Courtapps04	[redacted]	Court
Scabdc01	[redacted]	Backup Domain Server
Hp9ux2	[redacted]	Finance
Scasmart01	[redacted]	Smartstream Acct
Scaintranet	[redacted]	Intranet

Host Name	IP Address and Operating System	Critical Function
Snoopy	[redacted]	Web Server
Exch01	[redacted]	Exchange
Pwoodapps01	[redacted]	Class Application
Corpspdapps01	[redacted]	Police
Gismain	[redacted]	GIS

Table 2 lists the IP address ranges for the subnets included in the network-level assessment.

Table 2. Subnets Scanned for Network-level Vulnerabilities

IP Address Range	Physical Location
[redacted]	Scottsdale, AZ

1.3 Approach Summary

As shown in Figure 1, SNCi used automated information security tools and interviews to collected data on the systems and subnets listed in Section 1.2 and the information security controls in place. SNCi then analyzed the tool output results using SNCi and industry best practices.

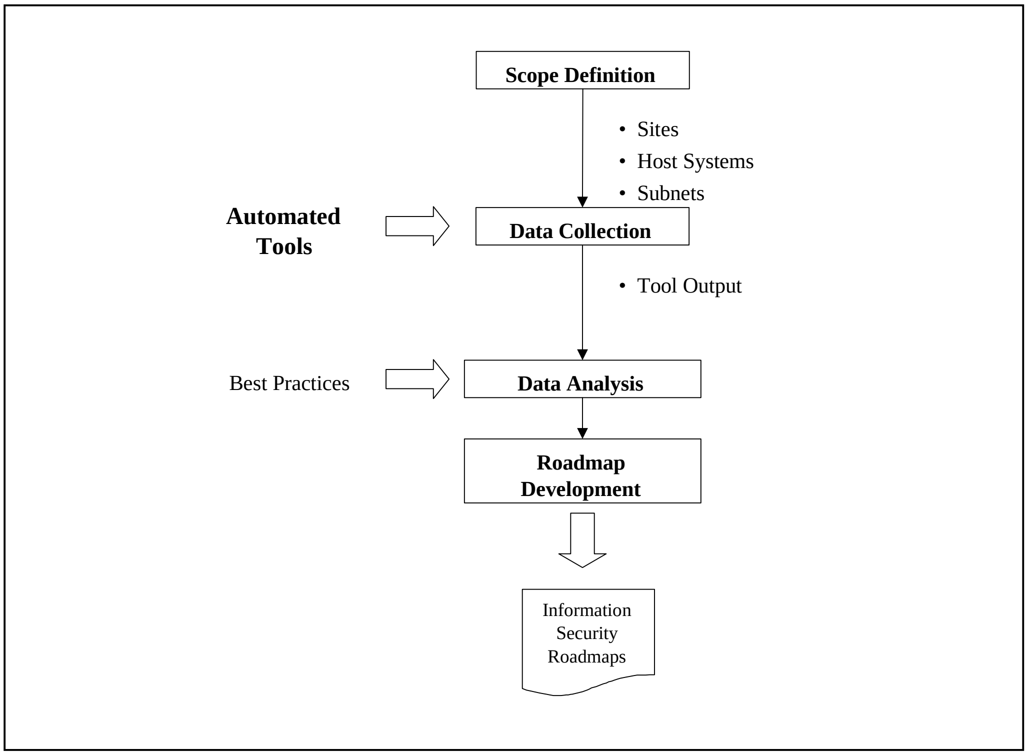

Figure 1. EVAS Process Overview

SNCi initially distilled the analysis results into an outbrief for the City of Scottsdale. After delivering the outbrief, SNCi began developing the Information Security

Solutions Roadmap. As described in Section 1.4, the Roadmap describes information security vulnerabilities discovered (including the actual product output as appendices), and presents prioritized recommendations for correcting assessed weaknesses.

1.4 Document Organization

The remainder of this document is organized as follows:

Section 2 summarizes SNCi's information security findings and recommendations for the City of Scottsdale. This section specifically addresses technical findings (from both external and internal perspectives).

Section 3 presents the SNCi-recommended information security solutions roadmap for addressing the findings and recommendation summarized in Section 2. The time-phased roadmap is structured to allow City of Scottsdale to achieve immediate improvements in the information security posture at the City of Scottsdale while implementing the plans necessary to address the wider range of information security issues identified in the EVAS review.

Appendix A describes the commercial information security tools used by SNCi and how these tools were configured. As described in this appendix, Enterprise Security Manager^{TM} was used to collect host-level data; NetRecon^{TM} was used to collect network-level data.

Appendix B contains detailed vulnerability findings tables that show the known vulnerability, solution, and individual devices where the vulnerabilities were found.

Appendix C references unprocessed product reports (raw data) and are provided on a CD that accompanies this report.

2. Findings and Recommendation Summary

Table 3 summarizes the information security ratings SNCi uses to describe information security assessment findings. These ratings describe an organization's information security posture relative to industry norms.

Table 3. Information Security Ratings

Rating	Definition
A	**Excellent** - Qualifies as an Information Security Best Practice
B	**Very Good** - Exceeds Industry Security Norms[1]
C	**Meets MINIMUM** Industry Security Norms
D	**Requires Improvements** to meet MINIMUM Industry Security Norms
F	**Unsatisfactory** - Well below Industry Security Norms

Overall Security Rating: D+

[1] Industry Security Norms are derived from SNCi's experience

Overall, SNCi determined that the effectiveness of the information security controls ir place at the City of Scottsdale is below industry norms.

SNCi reached this overall determination after assessing the City of Scottsdale from two perspectives:

1. External Connectivity and Systems Security
2. Internal Connectivity and Systems Security

Table 4 summarizes SNCi's assessment of the City of Scottsdale information security program in each of these areas.

Table 4. Information Security Ratings

Assessment Focus	Rating
External Connectivity and Systems Security	C-
Internal Connectivity and Systems Security	D

The following sections present specific information security findings and recommendations in each of the areas listed in Table 4. The following sections also include pointers to more detailed information.

2.1 External Connectivity and Systems Security

The External Connectivity and Systems Security area includes four major security domains.

1. Architecture
The architecture domain references any and all aspects of the underlying network systems. This will include revision and patch levels for the network hardware and software devices. A best practice network architecture would include the presence of network security appliances (.e.g. firewalls, routers, etc.), as well as the proper configuration of those appliances. Findings listed within this domain will contain references to the absence or misconfiguration of such devices.

2. Identification/Authentication
The identification and authentication domain references any and all methods to properly define which individual is accessing a network. The majority of network appliances currently use a username/password combination to properly identify authorized users. A best practice network identification/authentication would include two-factor authentication devices. Findings within this domain will include techniques to circumvent these methods, and/or impersonate an authorized user.

3. Access Control
The access control domain references any and all methods to access network appliances. Once identified, this domain determines the proper areas an authorized user can access. A best practice network access control would define at a minimum some discretionary control mechanism. Findings within this domain will include techniques to circumvent these network controls.

4. Accounting/Auditing

The accounting and auditing domain references any and all aspects to track and identify selected events within the network architecture. This will include any access attempt whether or not the attempt was successful. A best practice network accounting/auditing would include tracking unsuccessful attempts to authenticate to a network device. Findings within this domain will include failure to implement methods for tracking reasonable, network security events.

2.1.1 Notable Security Practices

The City of Scottsdale has taken some steps to provide network information security controls. The key step that the City of Scottsdale has taken is:

- Installed a firewall to provide protection from external unauthorized intrusion.

2.1.2 Assessed Weaknesses and Recommended Remedial Actions

Table 5 provides a high-level summary of weaknesses found by SNCi in the External Connectivity and Systems Security area.

Table 5. External Connectivity and Systems Security Weaknesses

Problem Area	Findings	Severit	High-level Remedial Action (Refer to detailed findings section)
Architecture	Configuration • Latest security patches are not installed • OS versions not at current level • Excessive services running	High	Install latest available vendor patches and upgrade OS versions to most current level. Review and stop unneeded services.
Identification and Authentication	Passwords • No passwords • Guessed passwords • Password filters not enabled	High	Develop a password policy, which includes the definition of a minimum and maximum password lifetime, minimum and maximum password length, and require the use of non-alphanumeric characters within the password.
Access Control	HP LaserJet printers w/o configuration passwords	High	Assign passwords to printers to prevent denial of service attacks.
Accounting and Auditing	None.		

2.2 Internal Connectivity and Systems Security

The Internal Connectivity and Systems Security area includes four major security domains.

1. Architecture
The architecture domain references any and all aspects of the underlying systems. This will include revision and patch levels for the server and workstation hardware and software devices. A best practice network architecture would include the implementation of the latest security patches, as well as the proper configuration of those systems. Findings listed within this domain will contain references to the misconfiguration of the servers and workstations.

2. Identification/Authentication
The identification and authentication domain references any and all methods to properly define which individual is accessing a server or workstation. The majority of systems currently use a username/password combination to properly identify authorized user. A best practice system identification/authentication would include two-factor authentication devices. Findings within this domain will include techniques to circumvent these methods, and/or impersonate an authorized user.

3. Access Control
The access control domain references any and all methods to access servers and workstations. Once identified, this domain determines the proper areas an authorized user can access. A best practice network access control would define at a minimum some discretionary control mechanism. Findings within this domain will include techniques to circumvent these host-based controls.

4. Accounting/Auditing
The accounting and auditing domain references any and all aspects to track and identify selected events within the server and workstation environment. This will include any access attempt whether or not the attempt was successful. A best practice system accounting/auditing would include tracking unsuccessful attempts to authenticate to a server or workstation. Findings within this domain will include not tracking system security events.

2.2.1 Notable Security Practices

The City of Scottsdale has taken some steps to provide system information security controls. The key steps that the City of Scottsdale has taken are:

- Major physical security measures including:
- Installation of cipher locks on the computer room,
- Use of userid and password authentication, and
- Consideration in purchasing security tools (e.g. ESM, NetRecon, ITA, and NetProwler) to assist with protection of the network.

2.2.2 Assessed Weaknesses and Recommended Remedial Actions

Table 6 provides a high-level summary of weaknesses found by SNCi in the Internal Connectivity and Systems Security area.

Table 6. Internal Connectivity and Systems Security Weaknesses

Problem Area	**Findings**	**Severity**	**High-level Remedial Action (Refer to Details Section of Report)**
Architecture	No Security Policies or Procedures	High	Create Information Security Policies, Standards and Procedures
	No Information Security Officer	High	Research and Hire an Information System Security Officer
	No Information Security Program	High	Implement an Information System Security Program
Identification and Authentication	User passwords Guessed. Examples include: • Guest • Arcada	High	Change the password.
	System allows blank passwords.	High	Enable passwords on all systems.
	No Account controls. Examples include: • No expiration dates • No lockout defined	High	Add account controls to systems.
	Accounts with No password. Example includes: • Guest	High	Create passwords for the identified accounts.
	Known accounts exist • Administrator • Guest	Medium	Rename or remove known accounts
Access Control	Excessive number of Users allowed to perform system functions. Examples include: • Shutdown computer • Change System time	Medium	Review users and remove users who do not need access to system services
Accounting and Auditing	Auditing not enabled	High	Enable the audit subsystems.
	Event log not protected	Medium	Protect the Event log so no one can overwrite it.

3. Information Security Solution Roadmap

This section presents the SNCi-recommended Information Security Solutions Roadmap for addressing the findings and recommendations summarized in Section 2. The time-phased Roadmap is structured to allow the City of Scottsdale to achieve immediate improvements in the information security posture while implementing the plans necessary to address the wider range of information security issues identified in the EVAS review.

3.1 Overview

The Roadmap presented in Sections 3.2 and 3.3 consists of two phases. Phase 1 (Section 3.2) has three categories of remedial actions to address the vulnerabilities summarized in Section 2:

1. Immediate Actions
2. Actions Within 30 Days
3. Actions Within 60 days

Phase 2 has two categories of remedial actions:

1. Actions Within 90 Days
2. Follow-on Actions

To develop the time-phased Roadmap, SNCi examined the vulnerabilities summarized in Section 2 and considered the appropriate timeframes for taking the recommended remedial actions (viewed as an integrated project). The resulting Roadmap approach, shown in Figure 2, sorts the High and Medium severity vulnerabilities into the appropriate Roadmap phase and category.

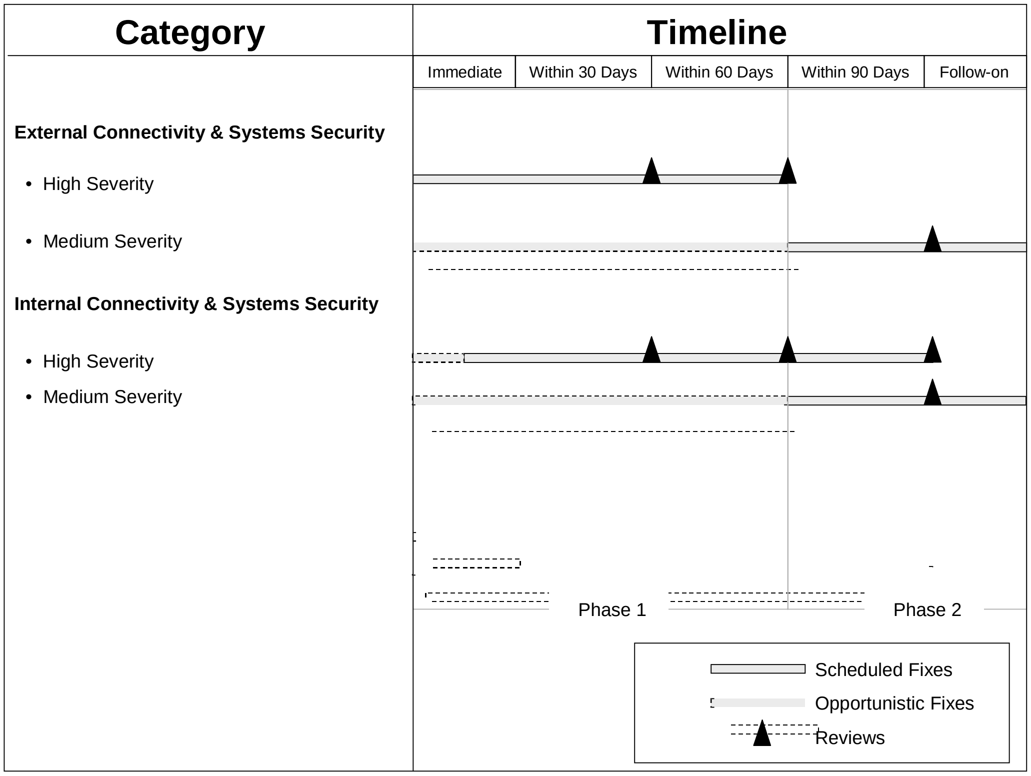

Figure 2. Roadmap Approach

For ease of reference, Table 7 summarizes the high severity vulnerabilities described in Section 2. Table 8 similarly summarizes the Medium severity vulnerabilities.

Table 7. High Severity Vulnerabilities

Assessment Perspective	Specific Vulnerability	High Level Remedial Action	Reference
External Connectivity and Systems Security	Configuration • Latest security patches are not installed • OS versions not at current level • Excessive services running	Install latest available vendor patches and upgrade OS versions to most current level. Review and stop unneeded services.	Table 5
	Passwords • No passwords • Guessed passwords • Password filters not enabled	Develop a password policy, which includes the definition of a minimum and maximum password lifetime, minimum and maximum password length, and require the use of non-alphanumeric characters within the password.	
	HP LaserJet printers w/o configuration passwords	Assign passwords to printers to prevent denial of service attacks.	
Internal Connectivity and Systems Security	User passwords Guessed. Examples include: • Guest • Arcada	Change the password.	Table 6
	No Security Policies or Procedures	Create Information Security Policies, Standards and Procedures	
	No Information Security Officer	Research and Hire an Information System Security Officer	
	No Information Security Program	Implement an Information System Security Program	
	System allows blank passwords.	Enable passwords on all systems.	
	No Account controls. Examples include: • No expiration dates • No lockout defined	Add account controls to systems.	
	Accounts with No password. Example includes: • Guest	Create passwords for the identified accounts.	
	Auditing not enabled	Enable the audit subsystems.	

Table 8. Medium Severity Vulnerabilities

Assessment Perspective	Specific Vulnerability	Medium Level Remedial Action	Reference
External Connectivity and Systems Security	None		
Internal Connectivity and Systems Security	Known accounts exist • Administrator • Guest	Rename or remove known accounts	Table 6
	Excessive number of Users allowed to perform system functions. Examples include: Shutdown computer Change System time	Review users and remove users who do not need access to system services	
	Event log not protected	Protect the Event log so no one can overwrite it.	

3.2 Phase 1 (60 Days)

As previously illustrated in Figure 2, Phase 1 of the Roadmap focuses on correcting High severity vulnerabilities. Specifically, Phase 1 will address:

- All of the High severity vulnerabilities discovered in the External Connectivity and Systems Security category.
- Many of the High Severity vulnerabilities discovered in the Internal Connectivity and Systems Security category.

SNCi recognizes that the City of Scottsdale also may be presented with opportunities to correct Medium severity vulnerabilities during the Phase 1 effort (as "targets of opportunity"). However, these Medium severity vulnerabilities should not be formally scheduled for completion until High severity vulnerabilities have been addressed to the maximum possible extent.

3.2.1 Immediate Actions

Table 9 lists the information security vulnerabilities that should corrected by the City of Scottsdale as soon as possible, on a highest priority basis.

Table 9. Immediate Actions.

Assessment Perspective	Specific Vulnerability	High Level Remedial Action	Reference	Detail Reference
External Connectivity and Systems Security	None		Table 5	
Internal Connectivity and Systems Security	No Information Security Officer	Research and Hire an Information System Security Officer	Table 6	
	User passwords Guessed. Examples include: • Guest • Arcada	Change the password.	Table 6	Section 5.1 Page 59
	System allows blank passwords.	Enable passwords on all systems.		Section 5.1 Page 60
	No Account controls. Examples include: • No expiration dates • No lockout defined	Add account controls to systems.		Section 5.1 Page 62, 84, 92, 95, 98
	Accounts with No password. Example includes: • Guest	Create passwords for the identified accounts.		Section 5.1 Pages 59, 61
	Auditing not enabled	Enable the audit subsystems.		Section 5.1 Pages 64, 66, 70 Section 5.2 Pages 136, 137, 142, 146

3.2.2 Actions Within 30 days

Table 10 lists the information security vulnerabilities that should corrected no later than 30 days after the Roadmap start.

Table 10. Actions Within 30 Days

Assessment Perspective	Specific Vulnerability	High Level Remedial Action	Reference	Detailed References
External Connectivity and Systems Security	Configuration • Latest security patches are not installed • OS versions not at current level • Excessive services running	Install latest available vendor patches and upgrade OS versions to most current level. Review and stop unneeded services.	Table 5	Section 5.1 Pages 65, 67, 69, 87, 89-91, 93 Section 5.2 Pages 99, 102-109, 112-135, 138-141, 145, 147-152, 154-159
	Passwords • No passwords • Guessed passwords • Password filters not enabled	Develop a password policy, which includes the definition of a minimum and maximum password lifetime, minimum and maximum password length, and require the use of non-alphanumeric characters within the password.		Section 5.1 Pages 59, 61
Internal Connectivity and Systems Security	No Security Policies or Procedures	Create Information Security Policies, Standards and Procedures	Table 6	
	No Information Security Program	Implement an Information System Security Program		

APPENDIX B

Management Response

MEMORANDUM

From: Carder W. Hunt, Chief Information Officer

To: Sonny Phillips, Assistant City Auditor
John Krusemark, Enterprise Technologist

C: Jennifer Jensen, Administrative Officer

Date: February 14, 2000

Subject: Management Response
Audit Number 9810.B
Internet Security Testing

Management Response: Information Systems management concurs with the findings and recommendations in this audit report. The security of the city's network is of fundamental importance, and we have already initiated some preliminary actions to address the findings of the consultant's study completed last November. As the audit correctly notes, Information Systems has prepared a budget request for a full-time security officer, as well as additional hardware and software to properly position the city organization to secure and protect its network.

Additional management responses will be forthcoming as this audit continues, and specific recommendations are made.

Carder W. Hunt, Chief Information Officer